타임스템프를 이용한 공증 보안메일 시스템

신동규* 서문석* 허원근* 임종인**

*시큐아이닷컴(주)

**고려대학교 정보보호연구소

Notarized Secure-Mail System Using Trust TimeStamp

Dong-gyu Shin* Moon-seog Seo* Weon-keun Huh* Jong-in Lim**

*SECUi.COM

**Center for Information Security Technologies(CIST), Korea University

요 약

본 논문에서는 전자메일에 보안기능과 공증기능을 함께 부여하는 방법에 대해 기술하고 있다. MIME(Multipurpose Internet Mail Extensions)[8]에 대하여 메시지의 무결성과 전자서명 생성 및 검증, 메시지의 암호화 및 복호화, 부인방지 기능을 지원하기 위해 S/MIME(Secure/Multipurpose Internet Mail Extensions)[1][2]을 적용하고 또한 문서에 대한 공증기능을 부여하기 위하여 서명 생성 후 오랜 기간 뒤에도 서명과 서명 생성 시 사용된 인증서의 유효성과 폐지여부를 검증 할 수 있도록 제 3 신뢰기관에 의해 발행된 Timestamp[7]를 적용하였다. 그리고 서명된 메일 형식에 receiptRequest[4] 식별자를 사용하여 수신자의 서명을 포함한 signed receipt[4]를 송신자에게 다시 보내게 하여 메일 수신여부를 검증 할 수 있도록 하였다.

I. 서론

인터넷과 컴퓨터의 보급으로 일상생활이나 업무에서도 전자메일을 많이 사용하고 있다. 전자메일의 편리함과 보편성 그리고 용이성 못지 않게 전자메일 취약성 부분도 크게 나타나고 있다. 전자메일의 송수신 시 메시지의 내용변조와 프라이버시 침해, 그리고 신분사칭이 용이하기 때문이다. 이를 방지하기 위해서 전송 메시지의 무결성과 송신자 인증, 메시지의 암호화 및 복호화, 부인방지 기능을 제공하는 S/MIME이 사용되고있다. 하지만 이것만으로는 공증 서비스 제공을 위해 필요한 서명생성 시의 서명 인증서의 유효성과 폐지 여부 그리고 서명 인증서가 폐지된 후에, 전자메일에 대한 서명의 유효성 여부를 판단 할 수 없다. 또한 발송된 전자메일의 수신 여부를 수신자가 부인했을 때 이것을 검증 할 방법이 없다. 본 논문에서는 제 3 신뢰기관에 의해 발행된 TimeStamp를 이용하여 오랜 기간동안 서명과 서명 인증서의 유효성 과 폐지여부를 검증 할 수 있도록 지원하고, S/MIME 기능 중 receiptRequest 속성을 이용하여 전자메일 수신자의 서명을 포함한 signed receipt를 송신자에게 보내게 하여 수신사실의 부인방지 기능을 지원 할 수 있도록 하여 공증서비스 제공을 위한 기본 보안요구사항을 충족할 수 있는 공증 보안메일 시스템을 제안한다.

II. 본문

1. 보안메일

보안메일이란 전자메일 전송프로토콜의 전송 메시지 규격인 MIME에 CMS(Cryptographic

Message Syntax)[3]구조체를 사용하여 MIME 메시지에 대한 서명 생성 및 검증, 암호화 및 복호화 기능을 첨가하여 전자우편을 안전하게 송수신할 수 있게 한다. 이를 S/MIME이라고 하며 S/MIME은 크게 서명과 암호화로 이루어진다.

1) 서명

MIME에 송신자의 비밀키로 서명을 생성한다. Application/pkcs7-mime[2] 의 signedData[3]를 사용하는 방법과 Multipart/signed[2]의 Application/pkcs7-signature[2]를 사용하는 방법이 있다.

2) 암호화

내용암호화 키를 생성하여 MIME을 암호화 한 후 내용암호화 키를 다시 수신자의 공개키로 암호화한다. Application/pkcs7-mime의 EnvelopedData [3]를 사용한다.

2. 부인방지 서비스를 위한 요구사항

부인방지서비스[6]란 서명 후에 독립적 검증자가 데이터에 유효한 인증서로 서명을 했는가를 알 수 있도록 증거를 제공하는 것을 의미한다. 부인방지는 공증서비스 제공을 위해서는 필수적으로 요구되는 서비스이다. 전자우편 서비스에서는 서명된 전자우편을 보내고, 수신한 사실을 부인하는 것을 방지하기 위한 증거를 제공하는 것이다.

1) 서명자의 요구조건

- 서명자는 반드시 서명과 서명에 사용된 인증서(인증서 정보)를 제출해야 한다.
- 서명자는 반드시 서명과 서명될 내용(내용정보)를 제출해야 한다.
- 서명자는 반드시 서명생성 시간을 가진다.
- 서명자는 반드시 서명될 내용 혹은 내용의 해쉬값을 가진다.

2) 서명검증자의 요구조건

- 검증자는 반드시 서명검증 전에 서명 인증서가 유효한가를 검증해야 한다.(CRL(Certificate Revocation List)[10], OCSP(Online Certificate Status Protocol)[9] 이용, 인증서 Path 검증)
- 검증자는 반드시 서명검증을 한다.
- 검증자는 서명자에게 receipt를 보낸다.

3. TimeStamping

TimeStamping[7]은 데이터와 시간을 암호학적으로 강하게 연관되도록 하는 것으로, 특정 시각점에 특정 데이터의 존재함을 증명하기 위해 사용된다. 특히, 서명 생성 후 인증서가 폐지되었을 때 그 서명에 대한 유효성을 검증 할 수 있도록 한다. 이를 위해서는 신뢰된 시각정보를 제공하는 제 3 신뢰기관(TSA : Time Stamp Authority)[7]이 있어야 한다. 이러한 신뢰기관으로부터 획득한 Timestamp는 공증서비스에서 요구되는 시간의 정확성에 대한 신뢰성을 부여 할 수 있다. TimeStamping은 크게 TSA에 시각정보를 요청하는 TimeStampReq[7]와 그에 대한 응답 메시지인 TimeStampResp[7]로 구성 되어있다. 데이터에 대한 서명의 유효성을 추후에 검증하기 위해 서명에 대한 TimeStamping도 지원한다. 응답메시지에는 시각정보를 포함한 TimeStampToken을 포함하여 보낸다. TimeStampToken은 CMS에서 정의한 SignedData형식에 따라 SignedData의 encap ContentInfo의 contentType에는 id-ct-TSTInfo[7]를 설정하고 content에는 TSTInfo[7]의 DER 인코딩 값을 넣는다.

4. 공증 보안메일용 속성(Attribute)

공증 보안메일 서비스를 위해 요구되는 여러 가지 속성들에 대해 정의한다.

1) Content Timestamp 속성

- Content Timestamp Attribute[5]는 서명 될 데이터에 대한 Timestamp로서 signed Attribute에 포함된다. 특정 시각점에 원본메시지의 존재여부를 증명하기 위해 사용된다.
- 속성형식 : id-aa-ets-contentTimestamp OBJECT IDENTIFIER [5]
- 속성값 : ContentTimestamp ::= TimeStampToken[7]

2) Signature Timestamp 속성

- Signature Timestamp Attribute[7]는 서명값에 대한 Timestamp로서 unsigned Attribute에 포함된다. 특정 시각점에 서명의 존재 여부를 증명하기 위해 사용된다. 서명 인증서 폐지 후에 서명의 유효성을 판별 할 수 있도록 한다.
- 속성형식 : id-aa-signatureTimeStampToken OBJECT IDENTIFIER [7]
- 속성값 : SignatureTimeStampToken ::= TimeStampToken

3) ES-C Timestamp 속성

● ES-C Timestamp Attribute[5]는 Type1 X-Timestamp 검증 데이터에 대한 Timestamp로서 unsigned Attribute에 포함된다. 특정 시각점에 서명과 서명 검증데이터의 존재 여부를 증명하기 위해 사용된다.

● 속성형식 : id-aa-ets-escTimeStamp OBJECT IDENTIFIER[5]

● 속성값 : ESCTimeStampToken ::= TimeStampToken

● TimeStampToken의 messageImprint[7]에는 type과 길이 정보를 제외한 서명값, 서명 TimeStampToken 식별자, 인증서정보 식별자, 폐지정보 식별자들을 연접한 값을 해쉬한 결과가 들어간다.

4) Time-Stamped Certificates and CRLs 속성

● Time-Stampes Certificates and CRLs Attribute[5]는 Type2 X-Timestamp validation 데이터에대한 Timestamp로서 unsigned Attribute에 포함된다. 특정 시각점에 검증자료의 존재여부를 증명하기 위해 사용된다.

● 속성형식 : id-aa-ets-certCRLTimestamp OBJECT IDENTIFIER [5]

● 속성값 : TimestampedCertsCRLs ::= TimeStampToken

● TimeStampToken의 messageImprint에는 type과 길이 정보를 제외한 인증서정보 식별자, v 폐지정보 식별자들을 연접한 값을 해쉬한 결과가 들어간다.

5) 인증서정보 속성

● Complete Certificate Refs Attribute[5]는 CA 인증서들의 관련정보(certHash, IssuerSerial)를 나타낸다. unsigned Attribute에 포함된다. 서명 인증서와 발급기관 인증서들의 참조정보를 제공한다.

● 속성형식 : id-aa-ets-certificateRefs OBJECT IDENTIFIER [5]

● 속성값 : CompleteCertificateRefs ::= SEQUENCE OF OTHERCertID[5]

6) 폐지정보 속성

● Complete Revocation Refs Attribute[5]는 인증서폐지여부 정보를 제공하는 CRL과 OCSP response의 관련정보를 나타낸다. unsigned Attribute에 포함된다. 인증서의 폐지여부에 사용된 CRL과 OCSP response의 참조정보를 제공한다.

● 속성형식 : id-aa-ets-revocationRefs OBJECT IDENTIFIER [5]

● 속성값 : CompleteRevocationRefs ::= SEQUENCE OF CrlOcspRef[5]

7) SigningCertificate 속성

● SigningCertificate Attribute[4]는 서명에 사용된 인증서를 나타내며, Substitute 공격과 re-Issue 공격을 방지하기 위해 사용되며 signed Attribute에 포함된다.

● 속성형식 : id-aa-signingCertificate OBJECT IDENTIFIER [4]

● 속성값 : SigningCertificate ::= SEQUENCE {

certs SEQUENCE OF ESSCertID,

policies SEQUENCE OF PolicyInformation OPTIONAL

}[4]

8) receiptRequest 속성

● receiptRequest Attribute[5]는 수신자에게 서명된 signed receipt를 요청할 때 사용되어 전자메일의 배달 확인에 사용되며 signed Attribute에 포함된다. 수신자가 전자메일의 수신을 거부 할 때 수신 여부를 증명 할 수 있게 한다.

● 속성형식 : id-aa-receiptRequest OBJECT IDENTIFIER [5]

● 속성값 : ReceiptRequest ::= SEQUENCE {

signedContentIdentifier ContentIdentifier,

receiptsFrom ReceiptsFrom,

receiptsTo SEQUENCE SIZE (1..ub-receiptsTo)) OF GeneralNames }[5]

5. 공증 보안메일 시스템의 처리흐름

다음은 공증 보안메일을 생성하는 방법을 나타낸 것이다. 공증 보안메일을 사용하려면 반드시 송신자의 서명이 필요하다.

1) 공증 보안메일의 송신

㉠송신 메시지 작성

전자메일 송신자가 수신자에게 보내고자 하는 내용을 작성한다. 첨부파일도 이 단계에서 첨부시킨다.

㉡메시지에 대한 Timestamp 생성.

전송 내용에 대한 무결성과 특정 시점에 대한 존재를 증명하기 위해 TSA에 Timestamp를 요청하여 Content Timestamp를 SignerInfo의 signed Attribute에 포함시킨다.

㉢서명자의 인증서 검증

전송 내용에 서명 할 서명자의 인증서의 유효성과 폐지여부를 검증한다. 폐지여부는 그림1 에 표기한 바와 같이 CRL이나 OCSP를 사용 할 수 있다. 검증이 성공해야만 서명을 할 수 있다. 서명 시점의 인증서의 유효성을 증명하기 위해 TSA에 Timestamp를 요청하여 서명 인증서에 대한 시점 확인을 받는다.

㉣인증서정보와 폐지정보 생성

서명 인증서의 path 검증에 사용된 CA 인증서의 관련 정보와 서명 인증서의 폐지여부 검증에 사용한 CRL과 OCSP response에 대한 관련정보를 각각 Complete Certificate Refs 식별자와 Complete Revocation Refs 식별자에 저장하여 SignerInfo의 unsigned Attribute에 포함시킨다.

㉤검증데이터의 Timestamp 생성

서명 인증서를 검증하는데 사용된 CRL 혹은 OCSP의 관련정보에 대하여 CA의 공모를 방지하기 위해 TSA에 Timestamp를 요청하여 TimestampedCertsCRLs를 SignerInfo의 unsigned Attribute에 포함시킨다.

㉥receiptRequest 생성

전자메일의 수신여부를 확인하기 위해 수신자의 서명이 담긴 signed receipt[4]를 요청하는 식별자를 signed Attribute에 포함시킨다.

㉦SigningCertificate 생성

서명에 사용된 인증서를 나타내고 Substitute 공격과 Re-issue 공격을 방지하기 위해 TSA에 Timestamp를 요청하여 SigningCertificate 식별자를 SignerInfo의 Signed Attribute에 포함시킨다.

㉧서명생성

서명 인증서에 대응하는 송신자의 비밀키로 전송 메시지의 해쉬값에 서명을 생성한다.

㉨서명에 대한 Timestamp 생성

서명의 유효성검증을 위해 TSA에 Timestamp를 요청하여 SignatureTimeStampToken를 SignerInfo의 unsigned Attribute에 포함시킨다.

㉩SignedData 생성

메시지의 무결성과 변조방지를 위해 CMS의 SignedData에 관련정보를 포함시킨다.

㉪S/MIME 메시지 전송

SignedData를 S/MIME형식으로 변환하여 수신자에게 전송한다.

2) 공증 보안 메일의 수신

㉠S/MIME 메시지 수신

수신된 S/MIME 메시지를 처리한다.

㉡송신자의 인증서 검증

수신자는 서명검증에 사용 할 송신자의 인증서(송신에의 ㉢부분)를 검증한다. SigningCertificate 식별자를 이용하여 서명 검증용 인증서를 확인하고 검증을 한다. 이때 path 검증도 포함한다.

㉢서명 검증

유효한 서명 인증서로 서명을 검증한다.

㉣signed receipt 생성 및 전송

서명이 확인된 후 receiptRequest 식별자가 포함된 경우, receipt를 생성하여 수신자의 서명을 포함한 signed receipt를 송신자에게 전송한다.

㉤S/MIME에서 전송 메시지 추출

서명이 검증이 성공되면, S/MIME에서 전송 메시지를 추출 할 수 있다.

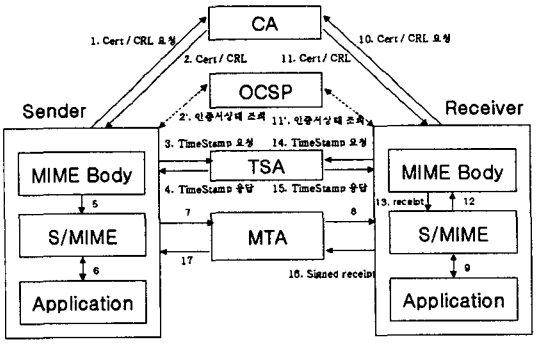

그림 1 : 공증 보안메일 송수신 흐름도

3) 중재자 (Arbitrator) 검증

● 전자메일 송신자와 수신자 사이의 분쟁이 발

생한 경우, 중재자인 제3자는 전송메일 내용과 receipt자료를 요청한다.

● 제3자는 전자메일에서 서명자인증서 혹은 인증서 관련정보, CA인증서 혹은 CA인증서 관련정보 그리고 폐지여부 관련정보를 추출하여 서명검증과 시각정보를 활용하여 정당한 전자메일인가를 확인 할 수 있다. 또한 receipt에는 전자메일 수신자의 서명이 포함되어 있으므로 수신확인 여부를 확인 할 수 있다.

6. 결론

일상생활이나 업무에 전자메일이 자주 사용하다 보면 증빙자료나 참고 자료로 전자메일을 편지함에 보관하는 일이 빈번하게 발생한다. 만일 중요 업무에 관련된 전자메일인 경우는 서명생성 후 많은 시간이 지난 뒤에 서명검증이 필요 할 수 있다. 기존의 S/MIME으로는 비록 서명시간을 나타내는 signingTime을 사용하여 서명의 생성 시간을 알 수 있었으나, 서명 당시의 서명 인증서의 폐지여부에 대한 정보는 알 수 없었다. 그러나 본 논문의 제안을 적용한 전자메일은 서명 생성 시간뿐 아니라, 서명 생성 시의 서명에 사용한 인증서와 인증서의 유효성과 폐지여부를 지원 할 정보에 대한 시각정보도 포함하고 있으므로 인증서가 폐지된 후 수년이 지난 후에도 당시의 서명이 유효함을 검증 할 수 있는 신뢰된 공증서비스 제공이 가능하다.

7. 참고문헌

[1] Ramsdell, B. , Editor, "S/MIME Version 3 Certificate Handling", RFC 2632, June, 1999.

[2] Ramsdell, B. , Editor, "S/MIME Version 3 Message Specification", RFC 2632, June, 1999.

[3] Housley, R. , "Cryptographic Message Syntax" RFC 2630, June 1999.

[4] P. Hoffman, Editor, "Enhenced Security Services for S/MIME" RFC 2634, June 1999.

[5] D. Pinkas and J. Ross and N. Pope "Electronic Signature Formats for long term electronic signatures" S/MIME Working Group, March 2001.

[6] T. Gindin, "Internet X.509 Public Key Infrastructure Technical Requirements for a non-Repudiation Service" PKIX Working Group, December 2000.

[7] C. Adams and P. Cain and D. Pinkas and R. Zuccherato "Internet X.509 Public Key Infrastructure Time Stamp Protocol" RFC 3161, August 2001.

[8] N. Freed and N. Borenstein, "Multipurpose Internet Mail Extension Part One : Format of Internet Message Bodies" RFC 2045, November 1996.

[9] M. Myers and R. Ankney and A. Malpani and S. Galperin and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol" RFC 2560, June 1999.

[10] R. Housley and W. Ford and W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" RFC 2459, January 1999.